SSI STRATEGIC STUDIES INSTITUTE
United States Army War College
&
UNITED STATES ARMY WAR COLLEGE PRESS

Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition Conference

March 4, 2013 | Dr. Robert J. Bunker

The "Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition" conference was held on November 1-2, 2012, in Pittsburgh, PA. The conference was sponsored by the Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh, and the Strategic Studies Institute of the U.S. Army War College, and co-sponsored by the National Cyber Forensic Training Alliance (NCFTA) and Indiana University of Pennsylvania (IUP). Sixty participants from academia, government, military, law enforcement, and private industry attended the multidisciplinary and policy-relevant gathering. Major themes identified in the agenda included:

- The spectrum of cyber threats that the United States increasingly must confront;
- The ways in which cyberspace is exploited by criminal and terrorist organizations; and,
- The evolution of cyberspace as an arena for strategic competition among the great powers.

The conference was composed of a welcome and introduction, three major panels, and a concluding round table on policy recommendations and responses. Acting conference chairs were Phil Williams, University of Pittsburgh; and John R. Deni, U.S. Army War College. Leading scholars, practitioners, and researchers who delivered presentations included Anna Aquilina, Serious Organised Crime Agency, UK; Stephen Blank, U.S. Army War College; Dave Bobrow, University of Pittsburgh; Nazli Choucri, MIT; William Claycomb, CERT, Carnegie Mellon University; Aaron Hackworth, Dell; Michael Kenney, University of Pittsburgh; Daniel Larkin, NCFTA; Martin Libicki, RAND; Michael McKeown, FBI; Isaac Porche, RAND; Harvey Rishikof, Drexel University; Jon Ruttencutter, DHS; Timothy Shimeall, CERT; Timothy Thomas, Foreign Military Studies Office; and William Waddell, U.S. Army War College.

Specific topics of interest included: the new realities of 21st century cyber politics and implications for the U.S. Department of Defense (DoD) and the U.S. interagency; internet futures; an internet of devices including three-dimensional printers (replicators); the legal dimensions of cyberspace; Chinese system sabotage; the use of botnets by Eastern European organized crime organizations; coordinated Russian and organized crime cyber operations; the indications and warnings that cybercrime has shifted to cyber conflict; cyber war by proxies and activists; deterrence in cyberspace, cyber defense, and public-private initiatives to mitigate and respond to cyber threats.

Major policy recommendations discussed during the course of the conference and summarized during the concluding round table included:

- Develop “rules of the road” for cyberspace, especially with countries such as China, to increase transparency and aid in avoiding miscalculations.
- Promote cooperative security efforts—including DoD-implemented security cooperation activities—in cyberspace between the United States and other governments.
- Maintain and grow public-private initiatives such as the NCFTA, to better integrate policies, procedures, and information sharing between and among government agencies such as DoD, the FBI, and private industry and academia.
- Promote university programs that seek to bridge the gaps between the technical, policy, practitioner, and legal worlds when it comes to cyber security—too often these worlds do not coordinate well with one another.
- Better define what we mean by the term cyberspace—for example, to clarify its functionality as only transmitting data or as something more encompassing in regards to dimensionality (e.g., virtual worlds).
- Reconsider the use of military models for characterizing and understanding cyberspace issues, perhaps by exploring public health (epidemiological) models for international coordination purposes.
- Develop standardized corporate “playbooks” concerning procedures and processes for responding to cyberspace based intrusions and criminal incidents.
- Review computer security lessons learned from private industry for their potential application to governmental and military environments.
- Have the Government Accountability Office (GAO) conduct a study on what is and is not

working with stakeholder computer systems.

- Determine strategies to help the U.S. Congress better create informed national cyberspace security legislation to protect the private sector specifically, and U.S. national security more broadly.

The full conference agenda can be accessed via the Matthew B. Ridgway Center website at *www.ridgway.pitt.edu*. A Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, edited volume composed of writings from this conference will be published in the future. It can be obtained upon publication at the Strategic Studies Institute website at *www.strategicstudiesinstitute.army.mil*.

*****

The views expressed in this Of Interest piece are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Govern-ment. This piece is cleared for public release; distribution is unlimited.

*****